

# Ranks of rational points of the Jacobian varieties of hyperelliptic curves

Bo-Hae Im and Byoung Du Kim

**ABSTRACT.** In this paper, we obtain bounds for the Mordell-Weil ranks over cyclotomic extensions of a wide range of abelian varieties defined over a number field  $F$  whose primes above  $p$  are totally ramified over  $F/\mathbb{Q}$ . We assume that the abelian varieties may have good non-ordinary reduction at those primes. Our work is a generalization of [6], in which the second author generalized Perrin-Riou's Iwasawa theory for elliptic curves over  $\mathbb{Q}$  with supersingular reduction ([10]) to elliptic curves defined over the above-mentioned number field  $F$ . On top of non-ordinary reduction and the ramification of the field  $F$ , we deal with the additional difficulty that the dimensions of the abelian varieties can be any number bigger than 1 which causes a variety of issues. As a result, we obtain bounds for the ranks over cyclotomic extensions  $\mathbb{Q}(\mu_{p^{\max(M,N)+n}})$  of the Jacobian varieties of *ramified* hyperelliptic curves  $y^{2p^M} = x^{3p^N} + ax^{p^N} + b$  among others.

## 1. INTRODUCTION

In this paper, we construct an (Iwasawa) theory in the spirit of [9] and [10], and obtain bounds for the Mordell-Weil ranks of abelian varieties. Our first model is Barry Mazur's work, [9], in which he studied abelian varieties  $A/F$  with good ordinary reduction at every prime of  $F$  above a prime  $p$ . Another model we follow closely is Perrin-Riou's work, [10], in which she studied elliptic curves defined over  $\mathbb{Q}$  with good supersingular reduction, and succeeded in overcoming many difficulties due to the supersingular reduction type.

To explain the relevance of their work to our work, suppose that  $A$  is an abelian variety defined over a number field  $F$ , and  $F_\infty$  is a  $\mathbb{Z}_p$ -extension of  $F$  (i.e.,  $\text{Gal}(F_\infty/F) \cong \mathbb{Z}_p$ ) for a prime  $p$ . When  $A$  has good ordinary reduction at every prime of  $F$  lying above  $p$  (i.e.,  $A$  has good reduction at such a prime, and its associated formal group is of multiplicative type), the celebrated work ([9]) provides a criterion for whether  $A(F_\infty)$  has a finite rank or not. It is a great example of the potential strength of Iwasawa Theory.

---

*Date:* February 28, 2017.

2010 *Mathematics Subject Classification.* Primary 11R23, 11G10.

Bo-Hae Im is supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2014R1A1A2053748).

Although a similar result is expected for abelian varieties generally regardless of the reduction type, how to prove it is not known in many cases if not in most cases. The main obstacle is that a formal group of non-multiplicative type does not admit a non-trivial universal norm.

One of the notable attempts in the case of the non-ordinary reduction was the aforementioned work of Perrin-Riou ([10]). Her insight was that we might be able to use Fontaine's theory of group schemes in a clever way to construct a series of local points which satisfy a certain norm relation (but do not constitute a universal norm).

In particular, she obtained that for an elliptic curve  $E/\mathbb{Q}$  with good supersingular reduction at  $p$ , if  $\mathbf{L}_\alpha \neq 0$  (which is the "algebraic"  $p$ -adic  $L$ -function she constructed), then

$$\text{corank}_{\mathbb{Z}_p} \text{Sel}_p(E/\mathbb{Q}_n) \leq (p-1)(p^{n-1} + p^{n-2} + \cdots + p^m) + C,$$

where  $C$  is some fixed constant, and  $n - m = \frac{n}{2} + O(1)$ . Most surprisingly, when  $a_p(E) = 1 + p - E(\mathbb{Z}/p\mathbb{Z}) = 0$ , she applied a more refined idea, and obtained that  $\text{rank}(E/\mathbb{Q}_\infty)$  is finite just as Mazur showed for  $E/\mathbb{Q}$  with good ordinary reduction at  $p$ . Now, we have a more sophisticated Iwasawa theory of S. Kobayashi ([7]) for  $E/\mathbb{Q}$  in the case of the cyclotomic  $\mathbb{Z}_p$ -extension of  $\mathbb{Q}$  (and also note F. Sprung's work, [11], which generalizes Kobayashi's work, which applies to most elliptic curves defined over  $\mathbb{Q}$ , to every elliptic curve defined over  $\mathbb{Q}$ ). The work close to our work in its subject matter is [3] (which crucially relied on [8]) which generalized the aforementioned results to abelian varieties in a context different from that of this paper.

Our goal is to generalize her work to abelian varieties over a number field  $F$  whose primes above  $p$  are totally ramified over  $F/\mathbb{Q}$ . We assume that the abelian varieties may have non-ordinary reduction at primes above  $p$  (but otherwise, have good reduction at every prime above  $p$ ). We use the ideas of the second author's earlier paper ([6]), in which he studied abelian varieties of dimension 1 (hence elliptic curves). Three main obstacles are the reduction type, the ramification of the field, and the dimensions of the abelian varieties. The last one is a new issue not covered by [6], and as we will argue, it is not a trivial one.

In [6], the second author found that by applying Fontaine's theory more rigorously and judiciously, Perrin-Riou's idea can be extended to elliptic curves  $A$  defined over totally ramified fields  $F$  (with emphasis on "*ramified*"). In the manner of Perrin-Riou, he constructed a  $p$ -adic power series  $\mathbf{L}_\alpha$  for a root  $\alpha$  of the characteristic of the Dieudonné module of  $A$  ( $\mathbf{L}_\alpha$  becomes an integral power series if  $\alpha$  is a unit), and showed that if it is not 0, then

$$\text{corank Sel}_p(A/F_n) \leq (p-1)(p^{n-1} + p^{n-2} + \cdots + p^m) + C,$$

where  $\lambda = v(\alpha)$ , and  $n - m = \lambda n + O(1)$ . Also, under some conditions, he generalized Kobayashi's theory to the above elliptic curves  $A$ . It should be seen as an effort to establish an Iwasawa theory that works well in a more general case.

In this paper, we generalize the result in [6] to abelian varieties of any dimension. (We keep the condition that every prime of  $F$  above  $p$  is totally ramified over  $F/\mathbb{Q}$ .) See Proposition 3.16 for our main statement. Since we study abelian varieties of any dimension, we have the following issues: Our group schemes can have “mixed reduction” (i.e., a mix of ordinary and non-ordinary reduction), and different generators of the Dieudonne module have different “minimal polynomials”, thus different series of local points we construct have different norm relations. This is all very different from abelian varieties of dimension 1 (i.e., elliptic curves) which has only two types of good reduction at a given prime: good ordinary, and good supersingular. And, their Dieudonne module is generated by one element over  $\mathbf{D}$ . Thus, we resort to a rather complicated construction in Section 2.

Our work involves constructing explicit logarithms, and as part of the work, we give an explicit and general definition of the constant term of the logarithm, without which the resulting local points do not satisfy the norm relations. One may define it as a number which happens to force the resulting local points to satisfy the norm relations, but our construction is more natural in the sense that it explains the rather mysterious existence of such constant terms.

As a result of our work, we obtain bounds for the Mordell-Weil ranks of abelian varieties in a wide range of cases. The bounds are given in terms of the dimension of the abelian varieties, and some other terms associated to their Dieudonne modules. In particular, for non-negative integers  $N$  and  $M$ , we consider the Jacobian variety of the hyperelliptic curve,

$$C_N : y^2 = x^{3p^N} + ax^{p^N} + b,$$

and the Jacobian variety of the curve,

$$C_{M,N} : y^{2p^M} = x^{3p^N} + ax^{p^N} + b.$$

For the lack of better words, we call  $C_{M,N}$  a *ramified hyperelliptic curve*. In the former, we suppose  $C_N$  is defined over  $F = \mathbb{Q}(\zeta_{p^N})$ , and in the latter, over  $F = \mathbb{Q}(\zeta_{p^M}, \zeta_{p^N})$ . In both, we let  $F_\infty = \mathbb{Q}(\zeta_{p^\infty})$ , and  $F_n$  be the field  $F \subset F_n \subset F_\infty$  so that  $\text{Gal}(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}$ . We let  $H$  be a number field so that every prime of  $H$  above  $p$  is unramified over  $H/\mathbb{Q}$ . (For example, we may assume  $H$  is the field of complex multiplication if the curve has complex multiplication.)

Suppose  $A$  is either the Jacobian variety of the curve above, or its dual abelian variety. We choose certain irreducible polynomials  $q_1(x), \dots, q_s(x)$  ( $s = \dim A \cdot [HF : \mathbb{Q}]$ ) which are associated to the Dieudonne modules of  $A$ , and choose a zero  $\alpha_i$  of each  $q_i(x)$ . (See the discussion after Assumption 4.4.) And, we construct the algebraic  $p$ -adic  $L$ -function  $\mathbf{L}_{\{\alpha_i\}_i}$  (see Definition 3.13). Its construction is necessarily more sophisticated than that of  $\mathbf{L}_\alpha$  in [6] because the Dieudonne module in this case has a higher dimension. In many ways, constructing  $\mathbf{L}_{\{\alpha_i\}_i}$  is pivotal to our study. Then we obtain:

**Theorem 1.1.** *Let  $\mathbf{A}' = \text{Hom}(\cup_n A[p^n], \mathbb{Z}_p(1))$  where  $\mathbb{Z}_p(1)$  is the Tate twist of the trivial representation  $\mathbb{Z}_p$ . (Equivalently,  $\mathbf{A}' = \cup_n A^\vee[p^n]$  where  $A^\vee$  is the dual abelian variety of  $A$ .) If  $\mathbf{L}_{\{\alpha_i\}_i} \neq 0$ , then for some fixed  $C$ ,*

$$\text{corank}_{\mathbb{Z}_p} \text{Sel}_p(\mathbf{A}'/H \cdot F_n) \leq \sum_{i=1}^s (p-1) \times (p^{n-1} + p^{n-2} + \cdots + p^{m_i}) + C,$$

as  $n$  varies, where  $n - m_i = \lambda_i n + O(1)$  and  $\lambda_i = v_p(\alpha_i)$ .

In particular, let  $\lambda$  be the maximum of  $\lambda_1, \dots, \lambda_s$ . Then we have the following.

- (a) *If  $A$  is the Jacobian variety  $J_N/F$  of  $C_N$ , or its dual abelian variety  $J_N^\vee$ , then for some fixed  $C$ ,*

$$\begin{aligned} & \text{corank}_{\mathbb{Z}_p} \text{Sel}_p(\mathbf{A}'/H \cdot F_n) \\ & \leq \frac{3p^N - 1}{2} \cdot [H \cdot F_n : \mathbb{Q}] \cdot (p-1) \times (p^{n-1} + p^{n-2} + \cdots + p^m) + C, \end{aligned}$$

as  $n$  varies, where  $n - m = \lambda n + O(1)$ .

- (b) *If  $A$  is the Jacobian variety  $J_{M,N}$  of  $C_{M,N}$ , or its dual abelian variety  $J_{M,N}^\vee$ , then*

- (i) *when  $M > N$ , for some fixed  $C$ ,*

$$\begin{aligned} & \text{corank}_{\mathbb{Z}_p} \text{Sel}_p(\mathbf{A}'/H \cdot F_n) \\ & \leq \left( 1 - 2p^M + \frac{3p^N(2p^M - 1) + p^M}{2} \right) \cdot [H \cdot F_n : \mathbb{Q}] \times (p-1) \\ & \quad \times (p^{n-1} + p^{n-2} + \cdots + p^m) + C, \end{aligned}$$

as  $n$  varies, where  $n - m = \lambda n + O(1)$ , and

- (ii) *when  $M \leq N$ , for some fixed  $C$ ,*

$$\begin{aligned} & \text{corank}_{\mathbb{Z}_p} \text{Sel}_p(\mathbf{A}'/H \cdot F_n) \\ & \leq \left( 1 - 2p^M + \frac{3p^N(2p^M - 1) + 2p^M - p^N}{2} \right) \cdot [H \cdot F_n : \mathbb{Q}] \times (p-1) \\ & \quad \times \{p^{n-1} + p^{n-2} + \cdots + p^m\} + C, \end{aligned}$$

as  $n$  varies where  $n - m = \lambda n + O(1)$ .

Theorem 1.1 follows from Proposition 3.16 and Lemma 4.1. As noted in [6],  $\mathbf{L}_{\{\alpha_i\}} \neq 0$  if  $\text{Sel}_p(\mathbf{A}'/H \cdot F_n)^\chi$  is finite for any  $n$  and any character  $\chi$  of  $\text{Gal}(H \cdot F_n/H \cdot F)$ .

Note that  $\text{End}_F(J_N)$  contains  $\mathbb{Z}[\zeta_{p^N}]$ , and  $\text{End}_F(J_{M,N})$  contains  $\mathbb{Z}[\zeta_{p^M}] \times \mathbb{Z}[\zeta_{p^N}]$ . It is illustrative that the bounds in Theorem 1.1 (a) and (b) are proportional to the ranks of  $\mathbb{Z}[\zeta_{p^N}]$  or  $\mathbb{Z}[\zeta_{p^M}] \times \mathbb{Z}[\zeta_{p^N}]$ . We note that the bounds in Theorem 1.1 are probably better than the bounds obtainable by previously known Iwasawa theory methods in our case.

## 2. CONSTRUCTING LOCAL POINTS OF GROUP SCHEMES OF HIGHER DIMENSION

For Fontaine's theory of group schemes over local fields, refer to the original reference [1], or [6]. We use the notations and definitions the second author used in [6] Section 3 (and we do not repeat them). As in [6], we may drop  $k$  from  $\mathbf{D}_k = W[\mathbf{F}, \mathbf{V}]$  if  $k = \mathbb{Z}/p\mathbb{Z}$ .

We recall the Dieudonne module  $M = M(G)$  of a group scheme  $G$  over a finite field  $k$ . Also recall that where  $K'$  is a (possibly ramified) extension of  $\mathbb{Q}_p$ ,  $G$  is a smooth group scheme over  $\mathcal{O}_{K'}$ , and  $G_{/k}$  is the reduced group scheme over the residue field  $k$ ,  $L \subset M(G_{/k})_{\mathcal{O}_{K'}}$  is the set of logarithms of  $G$ .

2.1. Let  $K'$  be a totally ramified extension of  $\mathbb{Q}_p$ , and  $G$  be a smooth formal group scheme over  $\mathcal{O}_{K'}$  whose reduction is also smooth. Let  $L$  and  $M$  be respectively the set of logarithms of  $G$ , and the Dieudonne module of  $G$ .

Assume that  $M$  is torsion-free. In this section, we study a method to generate local points of  $G$ .

Naturally, we will build on the ideas of [6], but working with formal groups of higher dimensions require new ideas. There are several issues. A lesser one is that  $M$  and  $L$  are not generated by one element. A bigger issue is that ordinary reduction types and non-ordinary reduction types are mixed in general, and cannot be easily separated to the best of our knowledge. The method for group schemes of dimension 1 would naturally extend to group schemes of any dimension if they are (over the given field) isogenous to products of group schemes of dimension 1. But every group scheme may not be of this kind. So, we need to develop a more sophisticated method.

Finally, unlike the dimension one case, each generator of  $M$  may have a different "minimal polynomial" (which we define later), and the minimal polynomial may not be irreducible.

We will present our solutions to these issues. First we note the following:

**Proposition 2.1.**  *$M \otimes \mathbb{Q}_p \cong (M^{ord} \otimes \mathbb{Q}_p) \times (M^{non-ord} \otimes \mathbb{Q}_p)$  for some finitely generated  $\mathbf{D}$ -modules  $M^{ord}$  and  $M^{non-ord}$  so that all the eigenvalues of  $\mathbf{F}$  acting on  $M^{ord}$  have valuation 1, and all the eigenvalues of  $\mathbf{F}$  acting on  $M^{non-ord}$  have valuation less than 1.*

*Proof.* Since  $\mathbf{FV} = p$ , and  $M$  is invariant under both  $\mathbf{F}$  and  $\mathbf{V}$ , the valuation of an eigenvalue of  $\mathbf{F}$  cannot be greater than 1.

We can find  $M^{ord}$ ,  $M^{non-ord}$  as follows: Let  $f(x) = (x \cdot 1 - \mathbf{F}|M) \in \mathbb{Z}_p[x]$ . Factorize  $f(x) = f_1(x)f_2(x)$  so that all the roots of  $f_1$  have valuation 1, and all the roots of  $f_2$  have valuation less than 1. It is clear that we can choose  $f_1$  and  $f_2$  such that they are monic and  $f_1, f_2 \in \mathbb{Z}_p[x]$ .

Then, we can choose modules  $M^{ord} = f_2(\mathbf{F})M$ , and  $M^{non-ord} = f_1(\mathbf{F})M$  which are clearly invariant under  $\mathbf{F}$ .

Since  $\mathbf{F}$  and  $\mathbf{V}$  are commutative (in fact,  $\mathbf{FV} = \mathbf{VF} = p$ ), both  $M^{ord}$  and  $M^{non-ord}$  are invariant under  $\mathbf{V}$  as well.  $\square$

By scaling if necessary, we can assume  $M \subset M^{ord} \times M^{non-ord}$ .

**Notation 2.2.** Let  $d$  be the dimension of  $G$ , and choose  $l_1, \dots, l_d \in L$  so that  $L$  is generated by them over  $\mathcal{O}_{K'}$ . We choose them in such a way that we can write

$$\begin{aligned} l_1 &= m'_1 + m''_1 \\ l_2 &= m'_2 + m''_2 \\ &\vdots \\ l_{d_1} &= m'_{d_1} + m''_{d_1} \\ l_{d_1+1} &= 0 + m''_{d_1+1} \\ &\vdots \\ l_d &= 0 + m''_d \end{aligned}$$

for  $m'_1, \dots, m'_{d_1} \in M^{ord}_{\mathcal{O}_{K'}}$  and  $m''_1, \dots, m''_d \in M^{non-ord}_{\mathcal{O}_{K'}}$ .

We also let  $d_2 = d - d_1$ .

**Definition 2.3.** Let  $L^{ord} = \mathcal{O}_{K'}(m'_1, \dots, m'_{d_1}) \subset M^{ord}_{\mathcal{O}_{K'}}$ . Recall the maximal ideal  $\mathfrak{m}'$  of  $\mathcal{O}_{K'}$ . We define  $G^{ord}$  as follows: For an  $\mathcal{O}_{K'}$ -algebra  $R$ ,  $G^{ord}(R)$  is the subgroup of  $G_{M,L}(R)$  given by the pull-back of the fiber product

$$\begin{array}{ccc} \text{Hom}(M^{ord}, CW_k(R/\mathfrak{m}'R)) & \longrightarrow & \text{Hom}(L^{ord}, (R \otimes \mathbb{Q}_p)/P'(R)) \\ & & \uparrow \\ & & \text{Hom}(L^{ord}, R \otimes \mathbb{Q}_p) \end{array}.$$

Here, the pull-back is given by  $M \rightarrow M^{ord} \times M^{non-ord} \rightarrow M^{ord}$  and  $L \rightarrow L^{ord}$  (the latter being given by  $l_1 \mapsto m'_1, l_2 \mapsto m'_2, \dots, l_{d_1} \mapsto m'_{d_1}, l_{d_1+1} \mapsto 0, \dots, l_d \mapsto 0$ ).

2.2. In this section, we let  $K$  be an unramified (finite) extension of  $\mathbb{Q}_p$ , and  $k$  be the field of residues of  $\mathcal{O}_K$ .

Let  $P(x) = b_d x^d + b_{d-1} x^{d-1} + \dots + b_0 \in \mathbb{Z}_p[x]$ , and suppose  $b_d$  is a unit, and all the zeros of  $P(x)$  have valuation greater than 0 and less than 1. (In fact,  $b_d$  will be always 1, but we keep  $b_d$  for readability.) Consequently,  $b_i/b_d \in p\mathbb{Z}_p$  ( $i = 0, \dots, d-1$ ), and  $p^i b_i/b_0 \in p\mathbb{Z}_p$  ( $i = 1, \dots, d$ ).

Suppose

$$f(X) = X^p + \alpha_{p-1} X^{p-1} + \dots + \alpha_1 X \in \mathcal{O}_K[X]$$

satisfies

$$p|\alpha_i \text{ for } i = 1, \dots, p-1, \text{ and } v_p(\alpha_1) = 1.$$

Let  $j(x) = P(x)/b_0 - 1 = \frac{b_d}{b_0}x^d + \frac{b_{d-1}}{b_0}x^{d-1} + \cdots + \frac{b_1}{b_0}x$ .

Later in this section, we will define  $j(\varphi)$  which imitates the properties of  $j(\mathbf{F})$ . But first, we make the following formal definition.

**Definition 2.4.** (1) Recall that  $b_d = 1$  and  $\mathbf{F}\mathbf{V} = \mathbf{V}\mathbf{F} = p$ . We define

$$\begin{aligned} j(\mathbf{F})^{-1} &= \left[ \frac{b_d}{b_0} \mathbf{F}^d \left( 1 + \frac{b_{d-1}}{b_d} \mathbf{F}^{-1} + \cdots + \frac{b_1}{b_d} \mathbf{F}^{d-1} \right) \right]^{-1} \\ &= b_0 \frac{\mathbf{V}^d}{p^d} \left( 1 + b_{d-1} \frac{\mathbf{V}}{p} + \cdots + b_1 \frac{\mathbf{V}^{d-1}}{p^{d-1}} \right)^{-1} \end{aligned}$$

where the last line is formally expanded by the Taylor series  $(1 + x)^{-1} = 1 - x + x^2 - \cdots$ .

(2) Let  $\sigma$  be the  $p$ -th Frobenius map on  $K$  (i.e.,  $\sigma(x) = x^p \pmod{p}$  for  $x \in \mathcal{O}_K$ ). Recall that  $\mathbf{V}x = px^{\sigma^{-1}}$  for every  $x \in K$ . For each  $n \in \mathbb{Z}$ , we define

$$\epsilon^{\sigma^n} = (-j(\mathbf{F})^{-1} + j(\mathbf{F})^{-2} - \cdots) \cdot \left( -\frac{\alpha_{p-1}^{\sigma^n}}{p} \right).$$

This definition of  $\epsilon^{\sigma^n}$  is somewhat similar to  $\lambda_n$  in [4] p.54 and (2.1) in [5] in the sense that they are all defined by infinite series of similar flavor (although naturally the definition in this paper is much more descriptive and general). However, we believe the definition in this space has much more explanatory power because it can explain the existence of such a constant fully, and also it seems to be defined more naturally.

**Proposition 2.5.**

$$\epsilon^{\sigma^n} + \frac{b_1}{b_0} \epsilon^{\sigma^{n+1}} + \cdots + \frac{b_d}{b_0} \epsilon^{\sigma^{n+d}} = \frac{\alpha_{p-1}^{\sigma^n}}{p}.$$

*Proof.* We observe

$$\begin{aligned} \epsilon^{\sigma^n} &= j(\mathbf{F})^{-1} \frac{\alpha_{p-1}^{\sigma^n}}{p} - j(\mathbf{F})^{-1} (-j(\mathbf{F})^{-1} + j(\mathbf{F})^{-2} - \cdots) \cdot \left( -\frac{\alpha_{p-1}^{\sigma^n}}{p} \right) \\ &= j(\mathbf{F})^{-1} \frac{\alpha_{p-1}^{\sigma^n}}{p} - j(\mathbf{F})^{-1} \epsilon^{\sigma^n}. \end{aligned}$$

Thus,

$$j(\mathbf{F}) \epsilon^{\sigma^n} = \frac{\alpha_{p-1}^{\sigma^n}}{p} - \epsilon^{\sigma^n},$$

thus

$$\begin{aligned} \frac{\alpha_{p-1}^{\sigma^n}}{p} &= (1 + j(\mathbf{F})) \epsilon^{\sigma^n} \\ &= \left(1 + \frac{b_1}{b_0} \mathbf{F} + \cdots + \frac{b_d}{b_0} \mathbf{F}^d\right) \epsilon^{\sigma^n}, \end{aligned}$$

and since  $\mathbf{F}^i \epsilon^{\sigma^n} = \epsilon^{\sigma^{n+i}}$ , our claim follows.  $\square$

**Definition 2.6.** We let  $\mathcal{P}_K$  be the set of power series  $\sum_{n=0}^{\infty} A_n x^n$  so that  $A_0$  and  $nA_n \in \mathcal{O}_K$  for  $n = 1, 2, \dots$

Recall that  $\sigma$  is the  $p$ -th Frobenius on  $K$ . Let  $\varphi_f$  be an operator on  $\mathcal{P}_K$  given by

$$\varphi_f \circ a = \sigma(a) \text{ for } a \in k, \quad \varphi_f \circ X = f(X).$$

Recall that  $\mathcal{P}_K/p\mathcal{O}_K[[x]] \cong \hat{C}W(k[[X]])$ . It is easy to see that  $\varphi_f$  on  $\mathcal{P}_K/p\mathcal{O}_K[[x]]$  is equivalent to  $\mathbf{F}$ . Similar to  $\log_{\mathcal{F}_{ss}}(x)$  in [7] p.15 (and also similar to  $l(x)$  in [6] in its precise form), we define:

**Definition 2.7.** We define  $l(x)$  by

$$l(x) = [1 - j(\varphi_f) + j(\varphi_f)^2 - \cdots] \circ x.$$

Readers can see that  $\epsilon^{\sigma^n}$  is formally defined as the expansion of  $l(x)$  to the minus direction, which may explain its somewhat mysterious properties.

**Proposition 2.8.**  $l(x)$  is well-defined (i.e., a convergent power series).

*Proof.* Recall that  $p^i b_i / b_0 \in p\mathbb{Z}_p$  for  $i = 1, \dots, d$ . The rest is clear.  $\square$

**Notation 2.9.** (a) Let  $\pi_0 = 0$ , and  $\pi_n$  for  $n \geq 1$  be non-zero so that

$$f^{\sigma^{-n}}(\pi_n) = \pi_{n-1} \text{ for } n = 1, 2, \dots$$

(b) Let  $\text{Tr}_{n/m}$  denote  $\text{Tr}_{K(\pi_n)/K(\pi_m)}$ .

(c) Let  $f^{(i)}(x)$  denote  $f^{\sigma^{i-1}} \circ \cdots \circ f^{\sigma} \circ f(x)$ .

**Proposition 2.10.** For any  $i$  with  $0 \leq i < d$ , we have

$$\begin{aligned} &b_0 \text{Tr}_{n/n-d} \left( \epsilon^{\sigma^{-n+i}} + (\varphi_{f^{\sigma^{-n}}}^i \circ l^{\sigma^{-n}})(\pi_n) \right) \\ &\quad + p b_1 \text{Tr}_{n-1/n-d} \left( \epsilon^{\sigma^{-n+1+i}} + (\varphi_{f^{\sigma^{-n+1}}}^i \circ l^{\sigma^{-n+1}})(\pi_{n-1}) \right) \\ &\quad + \cdots + p^d b_d \left( \epsilon^{\sigma^{-n+d+i}} + (\varphi_{f^{\sigma^{-n+d}}}^i \circ l^{\sigma^{-n+d}})(\pi_{n-d}) \right) = 0. \end{aligned}$$

*Proof.* First, we note

$$(\varphi_{f^{\sigma^{-n+j}}}^i \circ l^{\sigma^{-n+j}})(\pi_{n-j}) = l^{\sigma^{-n+i+j}} \left( f^{(i), \sigma^{-n+j}}(\pi_{n-j}) \right) = l^{\sigma^{-n+i+j}}(\pi_{n-i-j}).$$



Then, we note

$$\begin{aligned}
& \text{Tr}_{n/n-d} l^{\sigma^{-n+i}}(\pi_{n-i}) \\
&= \text{Tr}_{n/n-d} \left( [1 - j(\varphi) + j(\varphi)^2 - \dots] \circ x \right)^{\sigma^{-n+i}} \Big|_{x=\pi_{n-i}} \\
&= \text{Tr}_{n/n-d} \pi_{n-i} - \text{Tr}_{n/n-d} \left( j(\varphi) \circ [1 - j(\varphi) + j(\varphi)^2 - \dots] \circ x \right)^{\sigma^{-n+i}} \Big|_{x=\pi_{n-i}} \\
&= -p^{d-1} \alpha_{p-1}^{\sigma^{-n+i}} - \text{Tr}_{n/n-d} \left[ \frac{b_1}{b_0} l^{\sigma^{-n+i+1}}(f^{\sigma^{-n+i}}(x)) + \frac{b_2}{b_0} l^{\sigma^{-n+i+2}}(f^{(2),\sigma^{-n+i}}(x)) \right. \\
&\quad \left. + \dots + \frac{b_d}{b_0} l^{\sigma^{-n+i+d}}(f^{(d),\sigma^{-n+i}}(x)) \right]_{x=\pi_{n-i}} \\
&= -p^{d-1} \alpha_{p-1}^{\sigma^{-n+i}} - \left[ p \frac{b_1}{b_0} \text{Tr}_{n-1/n-d} l^{\sigma^{-n+i+1}}(\pi_{n-i-1}) \right. \\
&\quad \left. + p^2 \frac{b_2}{b_0} \text{Tr}_{n-2/n-d} l^{\sigma^{-n+i+2}}(\pi_{n-i-2}) + \dots + p^d \frac{b_d}{b_0} l^{\sigma^{-n+i+d}}(\pi_{n-i-d}) \right].
\end{aligned}$$

By Proposition 2.5 (replacing  $n$  with  $-n+i$ ) our claim follows.  $\square$

Note the role of  $\epsilon^{\sigma^n}$  in the argument.

We note that if  $b_0, b_1, \dots, b_d$  are in an unramified field larger than  $\mathbb{Q}_p$ , then the above argument does not work directly because they are not fixed by  $\sigma$ , and we may need to find an alternative argument, which is one of the reasons that we assume  $P(x) = b_d x^d + \dots + b_0 \in \mathbb{Z}_p[x]$ .

- Definition 2.11.** (1) Suppose  $M$  is a finitely generated  $\mathbf{D}$ -module, and there is a  $\mathbf{D}$ -homomorphism  $M \rightarrow M(\mathbf{m}) \oplus M^c(\mathbf{m})$  for some  $\mathbf{D}$ -modules  $M(\mathbf{m})$  and  $M^c(\mathbf{m})$  so that  $M(\mathbf{m}) = \mathbf{D} \cdot \mathbf{m}$  for some  $\mathbf{m}$ .
- (2) For any  $m \in M$ , the minimal polynomial of  $m$  over  $\mathbb{Q}_p$  is the monic polynomial  $P(x) \in \mathbb{Q}_p[x]$  with the smallest degree such that  $P(\mathbf{F})m = 0$ .
- (3) We assume the minimal polynomial of  $\mathbf{m}$  over  $\mathbb{Q}_p$  is  $P(x)$ .

Assuming  $\mathbf{F}$  is a topological nilpotent on  $M(\mathbf{m})$  (i.e.,  $\mathbf{F}^n \rightarrow 0$  as action on  $M(\mathbf{m})$  as  $n \rightarrow 0$ ), it is clear that  $\mathbb{Z}_p[\mathbf{F}]\mathbf{m}$  is a subgroup of finite index in  $M(\mathbf{m})$ .

**Remark 2.12.** If  $\mathbf{D}_k = W(k)[\mathbf{F}, \mathbf{V}]$  for  $k \neq \mathbb{Z}/p\mathbb{Z}$  so that  $W(k)$  is strictly bigger than  $\mathbb{Z}_p$ , then the above definition of a minimal polynomial may not make sense. For example, suppose that for some  $p(x) \in W(k)[x]$ ,  $p(\mathbf{F})\mathbf{m} = 0$ . Then, for some  $a \in W(k)$ ,  $p(\mathbf{F})(a\mathbf{m})$  may not be 0. This is another reason that we assume the group scheme is defined over a totally ramified local field (thus  $k = \mathbb{Z}/p\mathbb{Z}$ ).

Recall that  $K'$  is a totally ramified extension of  $\mathbb{Q}_p$ . (Thus,  $K'$  is linearly disjoint over  $\mathbb{Q}_p$  from  $K$ .) Recall  $L$  is a (free)  $\mathcal{O}_{K'}$ -submodule of  $M_{\mathcal{O}_{K'}}$ .

**Definition 2.13.** Assume  $P(x) \in \mathbb{Z}_p[X]$ , and all its roots have valuation less than 1, and all its coefficients except the leading coefficient are in  $p\mathbb{Z}_p$ .

(a) Recall the polynomial  $f(x)$ . Define  $l(x)$  associated to  $P(x)$  and  $f(x)$  as in Definition 2.7.

(b) Recall  $\overline{\mathcal{P}}_K = \mathcal{P}_K/p\mathcal{O}_K[[X]]$ .

Fix  $C \in \mathbb{Z}$  ( $C > 0$ ) so that  $C$  annihilates  $M(\mathbf{m})/\mathbb{Z}_p[\mathbf{F}]\mathbf{m}$ . For each  $n \geq \mathbb{Z}$ , define  $\mathbf{x}^{\sigma^n} \in \text{Hom}_{\mathbb{Z}_p[\mathbf{F}]}(M(\mathbf{m}) \oplus M^c(\mathbf{m}), \overline{\mathcal{P}})$  by

$$\begin{aligned} \mathbf{x}^{\sigma^n} : M(\mathbf{m}) \oplus M^c(\mathbf{m}) &\rightarrow \overline{\mathcal{P}} \\ \mathbf{m} &\mapsto C \cdot l^{\sigma^n}(x) \\ M^c(\mathbf{m}) &\mapsto 0 \end{aligned}$$

and expand linearly. (Expand  $\mathbb{Z}_p[\mathbf{F}]$ -linearly to  $\mathbb{Z}_p[\mathbf{F}]\mathbf{m}$ , and then to the entire  $M(\mathbf{m})$  by scaling, which is possible because  $\mathbb{Z}_p[\mathbf{F}]\mathbf{m}$  is a subgroup of  $M(\mathbf{m})$  of finite index.)

(c) Also, for each  $n \in \mathbb{Z}$ , define  $\tilde{\mathbf{x}}^{\sigma^n} \in \text{Hom}_{\mathbb{Z}_p}(M(\mathbf{m}) \oplus M^c(\mathbf{m}), \mathcal{P}_K)$  by

$$\tilde{\mathbf{x}}^{\sigma^n}(\mathbf{F}^k \mathbf{m}) = C \cdot \left( \epsilon^{\sigma^{n+k}} + \varphi_{f^{\sigma^n}}^k \circ l^{\sigma^n}(X) \right), \quad \text{for } k = 0, 1, \dots, d-1$$

and

$$\tilde{\mathbf{x}}^{\sigma^n} : M^c(\mathbf{m}) \mapsto 0,$$

and extend it linearly.

Clearly,  $\tilde{\mathbf{x}}^{\sigma^n}$  modulo  $p\mathcal{O}_K[[x]]$  is  $\mathbf{x}^{\sigma^n}$ .

Similar to [6] Notation 4.8, we define the following.

**Definition 2.14.** Choose generators  $\mathbf{l}_1, \dots, \mathbf{l}_d$  of  $L$ . Recall that  $L \subset M_{\mathcal{O}_{K'}}$ . Via  $M \rightarrow M(\mathbf{m}) \oplus M^c(\mathbf{m})$ , consider  $L$  as a submodule of  $(M(\mathbf{m}) \oplus M^c(\mathbf{m}))_{\mathcal{O}_{K'}}$ . For each  $h = 1, \dots, d$ , write

$$\mathbf{l}_h = (\mathbf{l}_{ij}^{(h)})_{(i,j) \in I_0} \in \varprojlim_{(i,j) \in I_0} \mathbf{m}^i \otimes M^{(j)},$$

$$\mathbf{l}_{ij}^{(h)} = \left( \sum_{k=0}^{d-1} \alpha_{k,ij}^{(h)} \mathbf{F}^k \mathbf{m}, m_2 \right) \in (\mathbf{m}^i \otimes M(\mathbf{m})^{(j)}) \oplus (\mathbf{m}^i \otimes M^c(\mathbf{m})^{(j)}),$$

where  $\sum_{k=0}^{d-1} \alpha_{k,ij}^{(h)} \mathbf{F}^k \mathbf{m} \in \mathbf{m}^i \otimes M(\mathbf{m})^{(j)}$ , and  $m_2 \in \mathbf{m}^i \otimes M^c(\mathbf{m})^{(j)}$ .

For each  $h = 1, 2, \dots, d$  and each  $(i, j) \in I_0$ , we can write

$$\mathbf{F}^j \left( \sum_{k=0}^{d-1} \alpha_{k,ij}^{(h)} \mathbf{F}^k \mathbf{m} \right) = \sum_{k=0}^{d-1} \beta_{k,ij}^{(h)} \mathbf{F}^k \mathbf{m}$$

for some  $\beta_k^{(ij)} \in C^{-1} \mathbf{m}^i$ . For each  $n \in \mathbb{Z}$ , we define  $\mathbf{y}^{\sigma^n} \in \text{Hom}_{\mathcal{O}_{K'}}(L, K'[[x]])$  by

$$\begin{aligned}
\mathbf{y}^{\sigma^n}(\mathbf{l}_h) &= C \cdot \left( \sum_{(i,j) \in I_0} \sum_{k=0}^{d-1} \beta_{k,ij}^{(h)} \tilde{\mathbf{x}}^{\sigma^n}(\mathbf{F}^k \mathbf{m}) \right) \\
&= C \cdot \left( \sum_{(i,j) \in I_0} \sum_{k=0}^{d-1} \beta_{k,ij}^{(h)} (\epsilon^{\sigma^{n+k}} + \varphi_{f^{\sigma^n}}^k \circ l^{\sigma^n}(X)) \right)
\end{aligned}$$

for each  $h = 1, \dots, d$ .

**Definition 2.15.** Recall Fontaine's map  $\omega$  and group  $P'$  which are defined as follows ([1] Chapter 2):  $\omega$  is given by

$$\begin{aligned}
\omega : \hat{C}W(g) &\rightarrow \mathbb{Q}_p \otimes g \\
(\dots, a_{-n}, \dots, a_{-1}, a_0) &\mapsto \sum_{n=0}^{\infty} p^{-n} a_{-n}^{p^n}.
\end{aligned}$$

And, for any  $\mathcal{O}_{K'}$ -algebra  $g$ ,  $P'(g)$  is an  $\mathcal{O}_{K'}$ -submodule of  $\mathbb{Q}_p \otimes g$  generated by  $p^{-n} a^{p^n}$  for all  $n \geq 0$  and all  $a \in \mathfrak{m}' \cdot g$  (you may also see [6] Definition 3.1 for a reference).

(a) Let  $G_{M(\mathbf{m}) \oplus M^c(\mathbf{m}), L}(\mathcal{O}_{K \cdot K'}[[x]])$  be the fiber product given by the following diagram

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathbb{Z}_p[\mathbf{F}]}(M(\mathbf{m}) \oplus M^c(\mathbf{m}), \hat{C}W(k[[x]])) & \xrightarrow{\omega} & \mathrm{Hom}_{\mathcal{O}_{K'}}(L, K \cdot K'[[x]]/P'(\mathcal{O}_{K \cdot K'}[[x]])) \\
& & \uparrow \\
& & \mathrm{Hom}_{\mathcal{O}_{K'}}(L, K \cdot K'[[x]]).
\end{array}$$

- (b) For each  $n \in \mathbb{Z}$ , let  $P^{\sigma^n} = (\mathbf{x}^{\sigma^n}, \mathbf{y}^{\sigma^n}) \in G_{M(\mathbf{m}) \oplus M^c(\mathbf{m}), L}(\mathcal{O}_{K \cdot K'}[[x]])$ . It is clear that  $P^{\sigma^n}$  is well-defined.
- (c) Note that there is a natural pull-back  $\iota : \mathrm{Hom}_{\mathbb{Z}_p[\mathbf{F}]}(M(\mathbf{m}) \oplus M^c(\mathbf{m}), \hat{C}W(k[[x]])) \rightarrow \mathrm{Hom}_{\mathbb{Z}_p[\mathbf{F}]}(M, \hat{C}W(k[[x]]))$ . Also, by Perrin-Riou's lemma (see the discussion [10] Section 3.1 right before Theorem 3.1), we have

$$\mathrm{Hom}_{\mathbb{Z}_p[\mathbf{F}]}(M, \hat{C}W(k[[x]])) \cong \mathrm{Hom}_{\mathbf{D}}(M, \hat{C}W(k[[x]])).$$

So, via the pull-back  $\iota$ , there is a map

$$G_{M(\mathbf{m}) \oplus M^c(\mathbf{m}), L}(\mathcal{O}_{K \cdot K'}[[x]]) \rightarrow G_{M, L}(\mathcal{O}_{K \cdot K'}[[x]]).$$

- (d) By abuse of notation, let  $P^{\sigma^n}$  denote the image of  $P^{\sigma^n}$  in  $G_{M, L}(\mathcal{O}_{K \cdot K'}[[x]])$  under this pull-back map.
- (e) Where  $Q \in G_{M, L}(\mathcal{O}_{K \cdot K'}[[x]])$  and  $\pi$  is an element in some local field with positive valuation, let  $Q(\pi) \in G_{M, L}(\mathcal{O}_{K \cdot K'}[\pi])$  denote  $Q$  with  $\pi$  substituted for  $x$ . Then, clearly  $P^{\sigma^n}(\pi_n) \in G_{M, L}(\mathcal{O}_{K \cdot K'}[\pi_n])$ .

Then, finally we obtain the following. (See [6] Proposition 4.10 for comparison.)

**Proposition 2.16.** *Recall  $P(x) = b_dx^d + \cdots + b_0$  to which the construction of  $P^{\sigma^n}$  is associated.*

*For each  $n \geq d$ , we have that modulo the torsions of  $G_{M,L}(\mathcal{O}_{K \cdot K'}[\pi_n])$ ,*

$$\sum_{s=0}^d p^s b_s \operatorname{Tr}_{n-s/n-d} P^{\sigma^{-n+s}}(\pi_{n-s}) = 0.$$

*Proof.* Since the equality is modulo torsions, we only need to check the “y” part. Then, the claim follows from Proposition 2.10.  $\square$

2.3. Recall that  $K$  is a (finite) unramified extension of  $\mathbb{Q}_p$ , and  $K'$  is a totally ramified extension of  $\mathbb{Q}_p$ . By the method in the previous section (Section 2.2), we can construct a series of local points satisfying a certain norm relation, and doing so does not require any condition on  $K'$  other than it being totally ramified over  $\mathbb{Q}_p$ .

However, we need to generate a sufficient number of series of local points, and we need to do so for a group scheme with a mix of ordinary reduction types and non-ordinary reduction types. In this subsection, we explain how to generate enough points, and to do so, we need to assume  $K'$  is generated by  $p^N$ -torsions of a certain Lubin-Tate group as below.

**Definition 2.17.** *Fix a uniformizer  $\rho$  of  $K$ .*

*Choose  $\zeta \in (\mathcal{O}_K^\times)_{\text{tor}}$  so that  $\mathbb{Z}_p[\zeta] = \mathcal{O}_K$ . For each  $i = 0, 1, \dots, [K : \mathbb{Q}_p] - 1$ , we choose*

$$f_i(x) = x^p + \alpha_{i,p-1}x^{p-1} + \cdots + \alpha_{i,1}x$$

*so that  $\alpha_{i,1}, \dots, \alpha_{i,p-1} \in p\mathcal{O}_K$ , and*

$$\alpha_{i,p-1} = \zeta^i p, \quad \alpha_{i,1} = \rho.$$

*For each  $i = 0, 1, \dots, [K : \mathbb{Q}_p] - 1$ , we let  $\pi_{i,0} = 0$ , and choose non-zero  $\pi_{i,n}$  for each  $n \geq 1$  so that*

$$f_i^{\sigma^{-n}}(\pi_{i,n}) = \pi_{i,n-1}.$$

*By the local class field theory,  $K(\pi_{i,n})$  does not depend on  $i$ . We let  $K(\pi_n)$  denote any  $K(\pi_{i,n})$ , and  $K(\pi_\infty)$  denote  $\cup_n K(\pi_n)$ .*

**Assumption 2.18.** *We suppose  $K' \cdot K = K(\pi_N)$  for some  $N$ .*

For example, we can consider the case  $K' = \mathbb{Q}_p(\pi_{p^N})$  for some  $N$ , and  $K$  is the unique unramified quadratic extension of  $\mathbb{Q}_p$ . One thing to note is that contrary to its appearance,  $K'$  is not an extension of  $K$  unless  $K = \mathbb{Q}_p$  because  $K'$  is totally ramified over  $\mathbb{Q}_p$ , and  $K$  is unramified over  $\mathbb{Q}_p$ .

Recall that **minimal polynomial** of  $\mathbf{m} \in M$  is the (non-zero) monic polynomial  $p(x) \in \mathbb{Q}_p[x]$  of minimal degree so that  $p(\mathbf{F})\mathbf{m} = 0$ .

**Notation 2.19.** Recall that  $G$  is a (smooth) formal group scheme over  $\mathcal{O}_{K'}$  of dimension  $d$ , and  $M$  is the associated Dieudonne module. From Section 2.1, recall the definitions of  $M^{\text{ord}}$  and  $M^{\text{non-ord}}$ . As in that section, let  $d_1$  and  $d_2$  be the minimum numbers of  $\mathbb{Q}_p[\mathbf{F}]$ -generators of  $M^{\text{ord}} \otimes \mathbb{Q}_p$  and  $M^{\text{non-ord}} \otimes \mathbb{Q}_p$ , respectively. (Then,  $d = d_1 + d_2$ .)

- (a) Choose generators  $\tilde{\mathbf{m}}_1, \dots, \tilde{\mathbf{m}}_{d_2}$  of  $M^{\text{non-ord}}$ , and by multiplying some polynomials (with coefficients in  $\mathbb{Q}_p$ ) of  $\mathbf{F}$  to them if necessary, obtain  $\mathbf{m}_1, \dots, \mathbf{m}_{d_2}$  so that their minimal polynomials are irreducible over  $\mathbb{Q}_p$ .
- (b) Let  $p_i(x) \in \mathbb{Z}_p[x]$  ( $i = 1, \dots, D$ ) be the minimal polynomial of  $\mathbf{m}_i$ . We write

$$p_i(x) = b_{d_i}^{(i)} x^{d_i} + b_{d_i-1}^{(i)} x^{d_i-1} + \dots + b_0^{(i)}.$$

(In fact,  $b_{d_i}^{(i)} = 1$  by definition, but for simplicity, we keep  $b_{d_i}^{(i)}$ .) By the definition of  $M^{\text{non-ord}}$ ,  $b_0^{(i)}, \dots, b_{d_i-1}^{(i)} \in p\mathbb{Z}_p$ .

By the definition of  $M^{\text{non-ord}}$ , it is clear that all the roots of  $p_i(x)$  have valuation less than 1.

**Definition 2.20.** For  $i = 0, 1, \dots, [K : \mathbb{Q}_p] - 1$  and  $j = 1, 2, \dots, d$ , we define the following: For each  $i$ , and every  $n \in \mathbb{Z}$ , we define  $\varphi_{f_i^{\sigma^n}}$  acting on  $\mathcal{P}_K$  by

$$\varphi_{f_i^{\sigma^n}} \circ a = \sigma(a) \text{ for } a \in k, \text{ and } \varphi_{f_i^{\sigma^n}} \circ X = f_i^{\sigma^n}(X).$$

For each  $j = 1, \dots, d_2$ , write  $J_j(x) = p_j(x)/b_0^{(j)} - 1$ . As in Definition 2.7, we define

$$l_{f_i, p_j}(x) = [1 - J_j(\varphi_{f_i}) + J_j(\varphi_{f_i})^2 - \dots] \circ x.$$

Also, for each  $k \in \mathbb{Z}$  we define  $\epsilon_{f_i, p_j}^{\sigma^k}$  attached to  $f_i, p_j$  by the method of Definition 2.4.

- (a) Let  $M(\mathbf{m}_j) = \mathbf{D} \cdot \mathbf{m}_j$ , and  $M^c(\mathbf{m}_j) = \prod_{i \neq j} \mathbf{D} \cdot \mathbf{m}_i \times M^{\text{ord}}$ . (See Notation 2.11.) Then, there is a canonically defined  $\mathbf{D}$ -homomorphism  $M \rightarrow M(\mathbf{m}_j) \oplus M^c(\mathbf{m}_j)$ .
- (b) As in Definition 2.13, fix a sufficiently large integer  $c > 0$  so that  $c$  annihilates  $M(\mathbf{m}_j)/\mathbb{Z}_p[\mathbf{F}] \cdot \mathbf{m}_j$  for every  $j$ , and for each  $n \in \mathbb{Z}$ , define  $\mathbf{x}_{f_i, p_j}^{\sigma^n} \in \text{Hom}_{\mathbb{Z}_p[\mathbf{F}]}(M, \overline{\mathcal{P}})$  by

$$\begin{aligned} \mathbf{x}_{f_i, p_j}^{\sigma^n} : M &\rightarrow \overline{\mathcal{P}} \\ \mathbf{m}_j &\mapsto c \cdot l_{f_i, p_j}^{\sigma^n}(x) \\ m(\in M^c(\mathbf{m}_j)) &\mapsto 0 \end{aligned}$$

and extend it  $\mathbb{Z}_p[\mathbf{F}]$ -linearly (which is possible because  $c$  annihilates  $M(\mathbf{m}_j)/\mathbb{Z}_p[\mathbf{F}] \cdot \mathbf{m}_j$ ).

Also, for each  $n \in \mathbb{Z}$ , define  $\tilde{\mathbf{x}}_{f_i, p_j}^{\sigma^n} \in \text{Hom}_{\mathbb{Z}_p}(M, \mathcal{P}_K)$ :

$$\tilde{\mathbf{x}}_{f_i, p_j}^{\sigma^n}(\mathbf{F}^k \mathbf{m}_j) = c \cdot \left( \epsilon_{f_i, p_j}^{\sigma^k} + \varphi_{f_i}^k \circ l_{f_i, p_j}^{\sigma^n}(X) \right), \text{ for } k = 0, 1, \dots, d_j - 1,$$

and

$$\tilde{\mathbf{x}}_{f_i, p_j}^{\sigma^n}(m) = 0 \text{ for } m \in M^c(\mathbf{m}_j).$$

Then, define  $\mathbf{y}_{f_i, p_j}^{\sigma^n}$  as in Definition 2.14 using  $\tilde{\mathbf{x}}_{f_i, p_j}^{\sigma^n}$ .

(c) Define  $P_{f_i, p_j}^{\sigma^n} = (\mathbf{x}_{f_i, p_j}^{\sigma^n}, \mathbf{y}_{f_i, p_j}^{\sigma^n}) \in G_{L, M(\mathbf{m}_j) \times M^c(\mathbf{m}_j)}(\mathcal{O}_{K \cdot K'}[[x]])$ . (See Definition 2.15 for the definition of  $G_{L, M(\mathbf{m}_j) \times M^c(\mathbf{m}_j)}(\mathcal{O}_{K \cdot K'}[[x]])$ .)

Via  $M \rightarrow M(\mathbf{m}_j) \oplus M^c(\mathbf{m}_j)$ , there is a natural homomorphism  $G_{L, M(\mathbf{m}_j) \oplus M^c(\mathbf{m}_j)} \rightarrow G_{L, M}$ . By combining with the isogeny  $G_{L, M} \rightarrow G$ , we obtain a homomorphism  $\varrho_j : G_{L, M(\mathbf{m}_j) \oplus M^c(\mathbf{m}_j)} \rightarrow G$ .

**Definition 2.21.** For each  $f_i$  for  $i = 0, 1, \dots, [K : \mathbb{Q}_p] - 1$ ,  $p_j$  for  $j = 1, \dots, d_2$ , and  $n \in \mathbb{Z}$ , we let

$$Q_{f_i, p_j}^{\text{non-ord}, \sigma^{-(N+n)}}(\pi_{i, N+n}) = \varrho_j(P_{f_i, p_j}^{\sigma^{-(N+n)}}(\pi_{i, N+n})) \in G(\mathcal{O}_K[\pi_{N+n}]).$$

Clearly,  $Q_{f_i, p_j}^{\text{non-ord}, \sigma^{-(N+n)}}(\pi_{i, N+n})$  should satisfy the relation in Proposition 2.10:

$$\begin{aligned} & b_0^{(i)} \text{Tr}_{N+n/N+n-d_i} Q_{f_i, p_j}^{\text{non-ord}, \sigma^{-(N+n)}}(\pi_{i, N+n}) \\ & + p b_1^{(i)} \text{Tr}_{N+n-1/N+n-d_i} Q_{f_i, p_j}^{\text{non-ord}, \sigma^{-(N+n-1)}}(\pi_{i, N+n-1}) \\ & + \dots + p^{d_i} b_{d_i}^{(i)} Q_{f_i, p_j}^{\text{non-ord}, \sigma^{-(N+n-d_i)}}(\pi_{i, N+n-d_i}) = 0 \end{aligned}$$

modulo torsions.

On the other hand, since  $G^{\text{ord}}$  is of multiplicative type with dimension  $d_1$ ,  $\varprojlim_n G^{\text{ord}}(\mathcal{O}_K[\pi_{N+n}])$  has rank  $d_1 \cdot [K \cdot K' : \mathbb{Q}_p]$ . In other words, we have the following:

**Proposition 2.22.** We can choose a set of elements  $\{(Q_{i, N+n}^{\text{ord}})_n\}_{i=1, 2, \dots, d_1 \cdot [K \cdot K' : \mathbb{Q}_p]}$  of  $\varprojlim_n G^{\text{ord}}(\mathcal{O}_K[\pi_{N+n}])$  so that it generates a free  $\mathbb{Z}_p[[\text{Gal}(K(\pi_\infty)/K(\pi_N))]]$ -submodule of rank  $d_1 \cdot [K \cdot K' : \mathbb{Q}_p]$ . In particular, we can choose them so that  $\{Q_{i, N+n}^{\text{ord}}\}_{i=1, 2, \dots, d_1 \cdot [K \cdot K' : \mathbb{Q}_p]}$  generates a subgroup of  $G^{\text{ord}}(\mathcal{O}_K[\pi_{N+n}])$  whose quotient has a bounded rank as  $n$  varies.

## 3. PERRIN-RIOU CHARACTERISTICS

The construction of local points in the previous section can be applied to the following setting:

**Notation 3.1.** *To simplify our assumptions, let  $F$  be a number field,  $F_\infty$  be its extension so that  $\text{Gal}(F_\infty/F) \cong \mathbb{Z}_p$ , and  $H$  be a number field so that every prime of it above  $p$  is unramified over  $H/\mathbb{Q}$ . For any prime  $\mathfrak{q}$  of  $H \cdot F_\infty$  above  $p$ , let  $\mathfrak{q}$  also denote  $\mathfrak{q} \cap H$  by abuse of notation, and let  $\mathfrak{p}$  denote both  $\mathfrak{q} \cap F_\infty$ , and  $\mathfrak{q} \cap F$  again by abuse of notation.*

**Assumption 3.2.** *For every prime  $\mathfrak{q}$  of  $HF_\infty$  above  $p$ ,  $(HF_\infty)_\mathfrak{q} = H_\mathfrak{q}(\pi_\infty)$  for the  $p$ -power torsions  $\pi_n$  of some Lubin-Tate group of height 1 defined over  $\mathcal{O}_{H_\mathfrak{q}}$  (equivalently,  $(HF_\infty)_\mathfrak{q}$  is abelian over  $\mathbb{Q}_p$ , and  $\text{Gal}((HF_\infty)_\mathfrak{q}/H_\mathfrak{q}) \cong \mathbb{Z}_p^*$ , and  $(HF)_\mathfrak{q} = H_\mathfrak{q}(\pi_{N_\mathfrak{q}})$  for some  $N_\mathfrak{q}$ ).*

There are some obvious cases where this assumption holds true: For example,  $F = \mathbb{Q}(\zeta_{p^N})$  for some  $N > 0$ ,  $F_\infty = \mathbb{Q}(\zeta_{p^\infty})$ , and  $H$  is a number field such that every prime of  $H$  above  $p$  is unramified over  $H/\mathbb{Q}$ .

**Notation 3.3.** *Let  $A$  be an abelian variety over  $F$  which has good reduction at every prime of  $F$  above  $p$ . Let  $A^\vee/F$  be its dual abelian variety.*

**Remark 3.4.** *It is probably difficult to determine whether a given abelian variety has good reduction at every prime or not. We believe that the result of this paper holds regardless of that. However, to the best of our knowledge, there is not a proper theory for abelian varieties which have bad (and non-multiplicative—in other words, unstable) reduction.*

**Notation 3.5.** *Let*

$$\Gamma = \text{Gal}(H \cdot F_\infty / H \cdot F) \cong \text{Gal}(F_\infty / F).$$

Let  $\mathcal{A}_\mathfrak{p}$  be the Neron model of  $A$  over  $\mathcal{O}_{F_\mathfrak{p}}$ , and let  $G_\mathfrak{p} = \varprojlim_n \mathcal{A}_\mathfrak{p}[p^n]$  (as the injective limit of finite group schemes). Let  $M_\mathfrak{p}$  be its Dieudonne module.

As in Proposition 2.1,  $M_\mathfrak{p} \otimes \mathbb{Q}_p$  has decomposition  $(M_\mathfrak{p}^{\text{ord}} \otimes \mathbb{Q}_p) \times (M_\mathfrak{p}^{\text{non-ord}} \otimes \mathbb{Q}_p)$ , and we may let  $d_\mathfrak{p}^{\text{ord}}$  be the number of generators of  $M_\mathfrak{p}^{\text{ord}}$ , and  $d_\mathfrak{p}^{\text{non-ord}}$  be the number of generators of  $M_\mathfrak{p}^{\text{non-ord}}$ .

Then, as in Definitions 2.20 and 2.21, there are

$$Q_{f_i, p_j}^{\text{non-ord}, \sigma^{-n}}(\pi_{i, N_\mathfrak{q}+n}) \in G(\mathcal{O}_{H_\mathfrak{q} F_\mathfrak{p}}(\pi_{N_\mathfrak{q}+n}))$$

for some  $f_i$ 's for  $i = 0, 1, \dots, [H_\mathfrak{q} : \mathbb{Q}_p] - 1$  and  $p_j$ 's for  $j = 1, \dots, d_\mathfrak{p}^{\text{non-ord}}$ , which we will not specify. Fix  $\tilde{\tau}_1, \dots, \tilde{\tau}_{[F_\mathfrak{p} : \mathbb{Q}_p]} \in \text{Gal}((HF_\infty)_\mathfrak{q} : H_\mathfrak{q})$  which lift all the elements of  $\text{Gal}((HF)_\mathfrak{q}/H_\mathfrak{q})$ . Then,  $Q_{f_i, p_j}^{\text{non-ord}, \sigma^{-n}}(\pi_{i, N_\mathfrak{q}+n})^{\tilde{\tau}_l}$  for all  $i, j, l$  give us  $d_\mathfrak{p}^{\text{non-ord}} \cdot [(HF)_\mathfrak{q} : \mathbb{Q}_p]$  points.

And, by Proposition 2.22, we can choose the following points:

**Definition 3.6.** We choose the points  $Q_{i,n}^{\mathfrak{q},ord} \in G(\mathcal{O}_{H_{\mathfrak{q}}F_{\mathfrak{q}}[\pi_{N_{\mathfrak{q}}+n}]})$  for  $i = 1, \dots, d_{\mathfrak{p}}^{ord} \cdot [(HF)_{\mathfrak{q}} : \mathbb{Q}_p]$  so that

$$N_{(HF)_{\mathfrak{q}}(\pi_{N_{\mathfrak{q}}+n+1})/(HF)_{\mathfrak{q}}(\pi_{N_{\mathfrak{q}}+n})} Q_{i,n+1}^{\mathfrak{q},ord} = Q_{i,n}^{\mathfrak{q},ord}.$$

We choose them so that  $\{Q_{i,n}^{\mathfrak{q},ord}\}_i$  generates a subgroup of  $G(\mathcal{O}_{H_{\mathfrak{q}}[\pi_{N_{\mathfrak{q}}+n}]})$  whose quotient has a bounded rank as  $n$  varies.

Altogether, we have  $d \cdot [(HF)_{\mathfrak{q}} : \mathbb{Q}_p]$  sequences of local points, and through all primes  $\mathfrak{q}$  of  $H \cdot F$  lying above  $p$ , we have  $d \cdot [HF : \mathbb{Q}]$  sequences of local points. For convenience, we list them  $\{Q_{i,n}\}_{i=1,\dots,d \cdot [HF:\mathbb{Q}]}$ .

Note that for each  $i$ ,  $\{Q_{i,n}\}_n$  satisfies

$$(1) \quad \sum_{s=0}^{e_i} g_s^{(i)} \text{Tr}_{n-e_i+s/n-e_i} Q_{i,n-e_i+s} = 0$$

modulo torsions for some irreducible  $q_i(x) = g_{e_i}^{(i)} x^e + \dots + g_0^{(i)} \in \mathbb{Z}_p[x]$ .

The following is a standard definition:

**Definition 3.7** (Relaxed Selmer groups). Let  $\mathbf{A}' = \cup_n A'^{\vee}[p^n]$ . For an extension  $L$  of  $F$ ,

$$\text{Sel}_{\text{rel}}(\mathbf{A}'/L) \stackrel{\text{def}}{=} \ker \left( H^1(L, \mathbf{A}') \rightarrow \prod_v \frac{H^1(L_v, \mathbf{A}')}{A'(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

where  $v$  runs over all primes of  $L$  not lying above  $p$ .

Clearly,  $\text{Sel}_{\text{rel}}$  satisfies the Control Theorem. (See [9],[2]. They assume that the abelian variety has good ordinary reduction at every prime above  $p$ , but their arguments can be easily adapted because  $\text{Sel}_{\text{rel}}$  is a relaxed Selmer group—in other words, it has no local condition for primes above  $p$ .) In other words,

$$\text{Sel}_{\text{rel}}(\mathbf{A}'/H \cdot F_n) \rightarrow \text{Sel}_{\text{rel}}(\mathbf{A}'/H \cdot F_{\infty})^{\text{Gal}(H \cdot F_{\infty}/H \cdot F_n)}$$

has finite and bounded kernel and cokernel as  $n$  varies.

Set

$$\Lambda \stackrel{\text{def}}{=} \mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[X]]$$

by choosing a topological generator  $\gamma$  of  $\Gamma$ , and setting  $\gamma = X + 1$ .

**Assumption 3.8.** Let  $M^{\vee}$  denote  $\text{Hom}(M, \mathbb{Q}/\mathbb{Z})$  (“the Pontryagin dual”). We assume

$$\text{rank}_{\Lambda} \text{Sel}_{\text{rel}}(\mathbf{A}'/H \cdot F_{\infty})^{\vee} = \dim A \cdot [H \cdot F : \mathbb{Q}].$$



As we can see easily by standard techniques of Iwasawa theory, this assumption is true if  $\text{Sel}(\mathbf{A}'/H \cdot F_n)^\chi$  is finite for any character  $\chi$  of  $\text{Gal}(H \cdot F_n/H \cdot F)$  for any  $n$ .

**Notation 3.9.** (1) For each  $n \geq 0$ , let

$$\Gamma_n = \Gamma/\Gamma^{p^n}, \quad \Lambda_n = \mathbb{Z}_p[\Gamma_n].$$

(2) For a group  $M$  on which  $\Gamma$  acts, we let

$$M_{/\Gamma^{p^n}} = M/\{(1-a) \cdot m \mid a \in \Gamma^{p^n}, m \in M\}.$$

Equivalently, where  $\gamma$  is a chosen topological generator of  $\Gamma$ ,

$$M_{/\Gamma^{p^n}} = M/(1 - \gamma^{p^n}) \cdot M.$$

**Definition 3.10.** (1) Let  $s = \dim A \cdot [H \cdot F : \mathbb{Q}]$ .

(2) Let

$$S_{\text{tor}} = (\text{Sel}_{\text{rel}}(\mathbf{A}'/H \cdot F_\infty)^\vee)_{\Lambda\text{-torsion}}.$$

If we assume Assumption 3.8, then there is a short exact sequence

$$(2) \quad 0 \rightarrow \text{Sel}_{\text{rel}}(\mathbf{A}'/H \cdot F_\infty)^\vee / S_{\text{tor}} \rightarrow \Lambda^s \rightarrow C \rightarrow 0$$

for a finite group  $C$ . This induces

$$\alpha'_n : \text{Sel}_{\text{rel}}(\mathbf{A}'/H \cdot F_n)^\vee \rightarrow \Lambda_n^s.$$

We note that there is a map

$$\beta_n : \prod_{\mathfrak{q}} A((HF_n)_{\mathfrak{q}}) \rightarrow \text{Sel}_{\text{rel}}(\mathbf{A}'/H \cdot F_n)^\vee$$

given by the local Tate duality.

**Definition 3.11.** (a) Let  $R_{i,n} \in \Lambda_n^s$  be the image of  $Q_{i,n}$  under  $\alpha'_n \circ \beta_n$ .

(b) Let  $\text{Proj}_n^m$  be the natural projection from  $\Lambda_m$  to  $\Lambda_n$  ( $m \geq n$ ).

Recall that each  $\{Q_{i,n}\}_n$  satisfies (1) for some  $q_i(x)$ .

In the following,  $\Lambda_\alpha$  denotes the set of power series  $f(T) \in \overline{\mathbb{C}}_p[[T]]$  satisfying  $|f(x)| < C|1/\alpha^n|$  for some fixed  $C > 0$  for every  $n \geq 1$  and  $x \in \mathbb{C}_p$  with  $|x| < |1/\sqrt[p^n]{p}|$ .

**Proposition 3.12.** For each root  $\alpha$  of  $q_i(x)$ , there is  $f_{\alpha,i} \in \Lambda_\alpha^s$  so that for some fixed constant  $c$ ,

$$R_{i,n} \equiv \sum_{\alpha} f_{\alpha,i} \alpha^{n+1} \pmod{c^{-1}((T+1)^{p^n} - 1)\Lambda}$$

for every  $n$ .

*Proof.* As in [6] Lemma 4.26, this is due to [10] Lemme 5.3.  $\square$

**Definition 3.13.** *First, we choose a generator  $g_{\text{tor}} \in \Lambda$  of the characteristic ideal of  $(\text{Sel}_{\text{rel}}(\mathbf{A}/HF_{\infty})^{\vee})_{\Lambda\text{-torsion}}$ . Now, recall  $q_i(x)$  associated to  $\{Q_{i,n}\}_n$  (see the discussion before Definition 3.7). We choose a root  $\alpha_i$  of each  $q_i(x)$ . Then, we define*

$$\mathbf{L}_{\{\alpha_k\}} \stackrel{\text{def}}{=} g_{\text{tor}} \times \det[f_{\alpha_1,1}, \dots, f_{\alpha_s,s}].$$

**Remark 3.14.** *Readers may wonder why we do not define  $\mathbf{L}_{\alpha}$  for a single zero  $\alpha$  of  $q(x) = \prod_i q_i(x)$  as the second author did in [6]. That is because if we choose a single zero  $\alpha$  of one specific polynomial  $q_i(x)$ , and define  $\mathbf{L}_{\alpha}$  in the manner of [6], then it has the effect of negating all the local points  $\{Q_{j,n}\}_n$  with  $q_j \neq q_i$ . The next example will illustrate what we mean.*

*This was not an issue in [6] because it assumed that the abelian variety was one-dimensional, and therefore, there was only one polynomial  $q_1(x)$ .*

**Example 3.15.** *Suppose we have two sequences of points  $\{Q_n\}_n, \{Q'_n\}_n$  satisfying  $N_{n+1/n}Q_{n+1} = Q_n$ , and  $N_{n+1/n}Q'_{n+1} = 2Q'_n$ . Define  $R_n, R'_n \in \mathbb{Z}_p[\Gamma_n]^2$  as above. Then, their corresponding polynomials (again, as above) are  $x-1$  and  $x-2$ , thus the roots are 1, 2.*

*Note that  $q(x) = (x-1)(x-2) = x^2 - 3x + 2$ , and we observe,*

$$\begin{aligned} N_{n+2/n}Q_{n+2} - 3N_{n+1/n}Q_{n+1} + 2Q_n \\ = N_{n+1/n}(N_{n+2/n+1}Q_{n+2} - Q_{n+1}) - 2(N_{n+1/n}Q_{n+1} - Q_n) = 0, \end{aligned}$$

*and similarly*

$$N_{n+2/n}Q'_{n+2} - 3N_{n+1/n}Q'_{n+1} + 2Q'_n = 0,$$

*thus*

$$\begin{bmatrix} R_{n+2}^t \\ R_{n+1}^t \end{bmatrix} = \begin{bmatrix} 3 & -2 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} R_{n+1}^t \\ R_n^t \end{bmatrix} \pmod{(1+x)^{p^n} - 1},$$

$$\begin{bmatrix} R'_{n+2}{}^t \\ R'_{n+1}{}^t \end{bmatrix} = \begin{bmatrix} 3 & -2 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} R'_{n+1}{}^t \\ R_n{}^t \end{bmatrix} \pmod{(1+x)^{p^n} - 1}.$$

*Since  $\begin{bmatrix} 3 & -2 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}^{-1}$ , by the method of [10, Lemme 5.3], we have*

$$\begin{aligned}
\begin{bmatrix} f_1 \\ f_2 \end{bmatrix} &= \varprojlim \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}^{-1} \begin{bmatrix} R_{n+1}^t \\ R_n^t \end{bmatrix} \\
&= \varprojlim \begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} R_{n+1}^t \\ R_n^t \end{bmatrix} \\
&= \varprojlim \begin{bmatrix} -R_{n+1}^t + 2R_n^t & (\text{mod } (1+x)^{p^n} - 1) \\ 0 \end{bmatrix},
\end{aligned}$$

and

$$\begin{aligned}
\begin{bmatrix} f'_1 \\ f'_2 \end{bmatrix} &= \varprojlim \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}^{-1} \begin{bmatrix} R'_{n+1}{}^t \\ R_n{}^t \end{bmatrix} \\
&= \varprojlim \begin{bmatrix} 0 \\ R'_{n+1}{}^t - R_n{}^t & (\text{mod } (1+x)^{p^n} - 1) \end{bmatrix}.
\end{aligned}$$

Note that if we were to define  $\mathbf{L}_\alpha$  as in [6], then  $\mathbf{L}_1 = g_{\text{tor}} \times \det[f_1, f'_1] = 0$ ,  $\mathbf{L}_2 = g_{\text{tor}} \times \det[f_2, f'_2] = 0$ , which are not meaningful.

Similarly with [6, Proposition 4.29], the next proposition follows from [10] Lemme 5.2, and the standard Iwasawa theory arguments, and this proves the first part of our main result, Theorem 1.1.

**Proposition 3.16.** *Recall  $s = \dim A \cdot [H \cdot F : \mathbb{Q}]$ . If  $\mathbf{L}_{\{\alpha_k\}} \neq 0$ , then for some fixed  $C$*

$$\text{corank}_{\mathbb{Z}_p} \text{Sel}_p(\mathbf{A}'/H \cdot F_n) \leq \sum_{i=1}^s (p-1) \times (p^{n-1} + p^{n-2} + \cdots + p^{m_i}) + C$$

where  $n - m_i = \lambda_i n + O(1)$  and  $\lambda_i = v_p(\alpha_i)$ .

Clearly,  $\text{rank } A'(H \cdot F_n)$  is not greater than  $\text{corank}_{\mathbb{Z}_p} \text{Sel}_p(\mathbf{A}'/H \cdot F_n)$  (and equal to it if the Shafarevich-Tate group is finite).

Also, as noted in [6],  $\mathbf{L}_{\{\alpha_k\}} \neq 0$  if  $\text{Sel}_p(\mathbf{A}'/H \cdot F_n)^\chi$  is finite for any  $n$  and any character  $\chi$  of  $\text{Gal}(H \cdot F_n/H \cdot F)$ .

#### 4. CERTAIN HYPERELLIPTIC CURVES AND THEIR JACOBIANS

In this section we consider the following types of hyperelliptic curves and investigate the bounds of ranks of their Jacobian varieties. We study the following setup which has a certain Iwasawa theory flavor. Let  $p > 3$  be a prime. For positive integers  $m$  and  $n$ , let

$$C_n : y^2 = x^{3p^n} + ax^{p^n} + b,$$

and

$$C_{m,n} : y^{2p^m} = x^{3p^n} + ax^{p^n} + b.$$

( $C_{m,n}$  is not a hyperelliptic curve. For convenience, we will call it a ramified hyperelliptic curve.) We compute the genera of  $C_n$  and  $C_{m,n}$  which are the dimensions of their jacobian varieties.

**Lemma 4.1.** *Denoting the genus of a curve  $C$  by  $g_C$ ,*

$$g_{C_n} = \frac{3p^n - 1}{2},$$

and

$$g_{C_{m,n}} = \begin{cases} 1 - 2p^m + \frac{3p^n(2p^m-1)+p^m}{2}, & \text{if } m > n \\ 1 - 2p^m + \frac{3p^n(2p^m-1)+2p^m-p^n}{2}, & \text{if } m \leq n. \end{cases}$$

*Proof.* By the Riemann-Hurwitz formula, for  $C_n$ , the degree of  $C_n$  to  $\mathbb{P}^1$  is 2 and the ramification index  $e$  is 2 at  $3p^n + 1$  points including at infinity. Hence it satisfies that

$$2g_{C_n} - 2 = 2(-2) + (3p^n + 1).$$

For  $C_{m,n}$ , the degree of  $C_{m,n}$  to  $\mathbb{P}^1$  is  $2p^m$ . If  $m \leq n$ , there are  $3p^n$  points not at infinity and they have ramification index  $e = 2p^m$ . And the ramification at infinity has the index  $e = 2$ . So

$$2g_{C_{m,n}} - 2 = 2p^m(-2) + (3p^n)(2p^m - 1) + p^m.$$

If  $m > n$ , similarly there are  $3p^n$  points not at infinity and they have ramification index  $e = 2p^m$ . And the ramification at infinity has the index  $e = 2p^{m-n}$ , so

$$2g - 2 = 2p^m(-2) + (3p^n)(2p^m - 1) + 2p^m - p^n.$$

□

Next we consider the endomorphism ring  $\text{End}(A)$  of an abelian variety  $A$ .

An abelian variety is isogenous to a product of simple abelian varieties. If  $A$  is a simple abelian variety, then  $\text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$  is a division ring. So, if  $A = A_1^{n_1} \times \cdots \times A_k^{n_k}$ , where  $A_k$ 's are simple and not isogenous to each other, then

$$\text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} = M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k),$$

for some division algebras  $D_i$ .

This only gives a rough upper bound for the size of the endomorphism ring. However, in the case of the Jacobian varieties of  $C_n$  and  $C_{m,n}$ , there is an obvious lower bound for the endomorphism rings.

Suppose  $C_n, C_{m,n}$  are defined over  $\mathbb{Q}(\zeta_{p^n})$  and  $\mathbb{Q}(\zeta_{p^m}, \zeta_{p^n})$  respectively. Let  $J_n$  (defined over  $\mathbb{Q}(\zeta_{p^n})$ ) be the Jacobian abelian variety of  $C_n$ , and  $J_{m,n}$  (defined over  $\mathbb{Q}(\zeta_{p^m}, \zeta_{p^n})$ ) be the Jacobian abelian variety of  $C_{m,n}$ .

Then,  $\text{End}_{\mathbb{Q}(\zeta_{p^n})} J_n$  contains  $\mathbb{Z}[\zeta_{p^n}]$  induced by the automorphisms of  $C_n$  given by  $(x, y) \mapsto (\zeta x, y)$  for any  $\zeta$  satisfying  $\zeta^{p^n} = 1$ , and  $\text{End}_{\mathbb{Q}(\zeta_{p^m}, \zeta_{p^n})} J_{m,n}$  contains  $\mathbb{Z}[\zeta_{p^m}] \times \mathbb{Z}[\zeta_{p^n}]$  induced by the automorphisms  $(x, y) \mapsto (\zeta x, \zeta' y)$  for any  $\zeta$  and  $\zeta'$  satisfying  $\zeta^{p^n} = 1$  and  $\zeta'^{p^m} = 1$ .

For the rest of the section, the abelian variety  $A/F$  is either  $J_n$  or  $J_{m,n}$ . If  $A = J_n$ , then the field  $F$  is  $\mathbb{Q}(\zeta_{p^n})$ , and if  $A = J_{m,n}$ , then  $F$  is  $\mathbb{Q}(\zeta_{p^n}, \zeta_{p^m})$ . In all cases,  $A^\vee/F$  is the dual abelian variety of  $A$ .

Let  $F_\infty = \mathbb{Q}(\zeta_{p^\infty})$ .

**Assumption 4.2.**  *$A/F$  has good reduction at the (unique) prime  $\mathfrak{p}$  of  $F$  above  $p$ .*

At the moment, we do not know whether Assumption 4.2 is true for  $J_n$ ,  $J_{m,n}$ , or their dual abelian varieties in general. We can only hope that it is often true. As mentioned earlier, we expect that the final result is probably true regardless. We hope that a proper theory for abelian varieties with bad reduction (especially unstable reduction) will be developed soon.

We let  $H$  be a number field so that every prime of  $H$  above  $p$  is unramified over  $H/\mathbb{Q}$ . Some choice of  $H$  might be more illuminating than others. For example, we may choose  $H$  so that  $A$  has “complex multiplication” over  $H$ : For instance, we may choose  $H = \mathbb{Q}(i)$  when  $p$  is an odd prime, and  $b = 0$ .

**Definition 4.3.** *Recall that  $A^\vee$  is the dual abelian variety of  $A$ . Also recall*

$$\mathbf{A} = \cup A[p^n], \quad \mathbf{A}' = \cup A^\vee[p^n],$$

where  $A^\vee$  is the dual variety of  $A$ . (In other words,  $\mathbf{A}' = \text{Hom}(\mathbf{A}, \mathbb{Z}_p(1))$ .)

Also, recall  $\Gamma = \text{Gal}(H \cdot F_\infty / H \cdot F)$ , and  $\Lambda = \mathbb{Z}_p[[\Gamma]]$  which we identify with  $\mathbb{Z}_p[[x]]$ .

**Assumption 4.4.** *Recall the relative Selmer group  $\text{Sel}_{\text{rel}}$  from Section 3. We assume  $\text{Sel}_{\text{rel}}(\mathbf{A}'/H \cdot F_\infty)$  has  $\Lambda$ -corank  $s = \dim A \cdot [H \cdot F : \mathbb{Q}]$ .*

As mentioned in Section 3, Assumption 4.4 is true if  $\text{Sel}_p(\mathbf{A}/H \cdot F_n)^\chi$  is finite for any  $n \geq 0$  and any character  $\chi$  of  $\text{Gal}(H \cdot F_n / H \cdot F)$ .

As in the discussion after Notation 3.5, for each prime  $\mathfrak{p}$  of  $F$  above  $p$ , define the Dieudonné module  $M_{\mathfrak{p}}$  associated to  $A/F_{\mathfrak{p}}$ . Also, as we did in the same discussion, construct local points  $\{Q_{i,n}\}_n$  for  $i = 1, \dots, \dim A \cdot [HF : \mathbb{Q}]$ , each associated to a monic irreducible polynomial  $q_i(x) \in \mathbb{Z}_p[x]$ .

The polynomials  $q_1, \dots, q_s$  depend on the choice of the above-mentioned local points. However, as we have demonstrated earlier, all of them are irreducible divisors of  $\det(x \cdot 1 - \mathbf{F}|M_{\mathfrak{p}})$  for some  $\mathfrak{p}$ , and every irreducible (polynomial) divisor of  $\det(x \cdot 1 - \mathbf{F}|M_{\mathfrak{p}})$  of any  $\mathfrak{p}$  is represented by them.

Then, by Proposition 3.16 and Lemma 4.1, we obtain Theorem 1.1.

## REFERENCES

- [1] J.-M. Fontaine, *Groupes  $p$ -divisibles sur les corps locaux*. Astérisque 47/48 (1977)
- [2] Ralph Greenberg, *Iwasawa theory for elliptic curves*. in Arithmetic Theory of Elliptic Curves, Volume 1716 of the series Lecture Notes in Mathematics, pp 51-144.

- [3] Kazim Buyukboduk, Antonio Lei, *Integral Iwasawa Theory of Galois Representations for non-ordinary primes*, to appear in Mathematische Zeitschrift.
- [4] Byoung Du Kim, *The parity conjecture for elliptic curves at supersingular reduction primes*. Compos. Math. 143 (2007), no. 1, 47-72.
- [5] -, *Signed-Selmer Groups over the  $\mathbb{Z}_p^2$ -extension of an Imaginary Quadratic Field* Canad. J. Math. 66(2014), 826-843
- [6] -, *Ranks of the Rational Points of Abelian Varieties over Ramified Fields, and Iwasawa Theory for Primes with Non-Ordinary Reduction*. Submitted, <https://arxiv.org/abs/1608.03315>.
- [7] Shin-ichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*. Invent. Math. 152 (2003), no. 1, 1-36.
- [8] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Coleman maps and the  $p$ -adic regulator*, Algebra Number Theory 5 (2011), no. 8, 1095-1131.
- [9] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*. Inventiones mathematicae, December 1972, Volume 18, Issue 3, pp 183–266.
- [10] Bernadette Perrin-Riou, *Theorie d'Iwasawa  $p$ -adique locale et globale*. Invent. math. 99, pp. 247–292 (1990).
- [11] Florian Sprung, *Iwasawa theory for elliptic curves at supersingular primes: A pair of main conjectures*. Journal of Number Theory Volume 132, Issue 7, July 2012, pp. 1483–1506.

DEPARTMENT OF MATHEMATICAL SCIENCES, KAIST, 291, DAEHAK-RO, YUSEONG-GU, DAEJEON, 34141, REPUBLIC OF KOREA  
*E-mail address:* `bhim@kaist.ac.kr`

SCHOOL OF MATHEMATICS AND STATISTICS, VICTORIA UNIVERSITY OF WELLINGTON, WELLINGTON 6140, NEW ZEALAND  
*E-mail address:* `byoungdu.kim@vuw.ac.nz`